Lecture 8.

We defined an algebraically closed field by the property: every polynomial of degree ≥ 1 has a root. In fact over an algebraically closed field F an arbitrary polynomial $f(t)$ of degree ≥ 1 can be decomposed as

$$f(t) = \alpha (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_d),$$

where $\alpha, \alpha_1, \dots, \alpha_d \in F$.

Let us prove it by induction on $\deg f(t)$.

If $\deg f(t) = 1$ then there is nothing to prove.

Let α_1 be a root of $f(t)$. Then

$$f_1(t) = (t-\alpha_1)\tilde{f}(t), \quad \deg \tilde{f} = \deg f - 1.$$

Applying the induction assumption to $\tilde{f}(t)$ we get the result.

<u>Question:</u> how can we check if all roots $\alpha_1, \alpha_2, \dots, \alpha_d$ are distinct?

Derivatives can be defined for polynomials over an arbitrary field.

Let $(t^n)' = n t^{n-1}$, $n \geq 0$,

and extend it to a linear transformation of $F[t]$:

$$\left(\sum \alpha_i t^i\right)' = \sum_i \alpha_i \cdot i \cdot t^{i-1}$$

The product rule still holds:

$$\left(f(t) g(t)\right)' = f'(t) g(t) + f(t) g'(t).$$

Suppose that $\alpha_1 = \alpha_2$, $f(t) = \alpha (t - \alpha_1)^2 \tilde{f}(t)$

Then $f'(t) = 2\alpha (t - \alpha_1) \tilde{f}(t) + \alpha (t - \alpha_1)^2 \tilde{f}(t)'$

We see that α_1 is a root of $f'(t)$, both polynomials $f(t)$ and $f'(t)$ are divisible by $t-\alpha_1$. Hence

$$\gcd(f(t), f'(t)) \neq 1.$$

Now suppose that all roots $\alpha_1, \ldots, \alpha_d$ are distinct. We will show that in this case $f(t)$ and $f'(t)$ do not have common roots.

$$f'(t) = \alpha(\widehat{t-\alpha_1})(t-\alpha_2)\cdots(t-\alpha_d) + \alpha(t-\alpha_1)(\widehat{t-\alpha_2})(t-\alpha_3)\cdots$$
$$\cdots(t-\alpha_d) + \cdots + \alpha(t-\alpha_1)\cdots(t-\alpha_{d-1})(\widehat{t-\alpha_d}).$$

Here $\wedge$ means that this factor is missing.

Now, $f'(\alpha_1) = \alpha(\alpha_1-\alpha_2)\cdots(\alpha_1-\alpha_d) \neq 0$

$f'(\alpha_2) = \alpha(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\cdots(\alpha_2-\alpha_d) \neq 0$

and so on.

Since $f(t)$ and $f'(t)$ do not have common roots we conclude:

all roots $\alpha_1, \ldots, \alpha_d$ are distinct if and only if $\gcd(f(t), f'(t)) = 1$.

Now we are ready to prove existence of fields of order p^n.

Let's start with the field $\mathbb{Z}(p)$. There exists an algebraically closed field K, such that the extension $K/\mathbb{Z}(p)$ is algebraic.

Consider the polynomial $t^{p^n}-t$. Since the field K is algebraically closed,

$$t^{p^n}-t=\alpha(t-\alpha_1)\cdots(t-\alpha_{p^n}).$$

<u>claim:</u> all roots $\alpha_1,\ldots,\alpha_{p^n}$ are distinct.

Indeed, $(t^{p^n}-t)'=p^n t^{p^n-1}-1=-1$ since $\operatorname{char} K=p$. The polynomial -1 does not have roots.

<u>claim:</u> $F=\{\alpha\in K \mid \alpha^{p^n}-\alpha=0\}=\{\alpha_1,\ldots,\alpha_{p^n}\}$ is a subfield of K.

We have to check all the conditions for a subfield.

Let $\alpha, \beta \in F$, that is, $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$.

Consider $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \sum_{i=1}^{p^n-1} \binom{p^n}{i} \alpha^i \beta^{p^n-i} + \beta^{p^n}$.

All binomial coefficients

$$\binom{p^n}{i}, \quad 1 \le i \le p^n - 1,$$

are divisible by p (Exercise!)

Hence $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$.

Furthermore,

$$(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha\beta$$

If $\alpha \neq 0$, then $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$!

We proved that F is indeed a subfield of K and $|F| = p^n$!

Existence of fields of order p^n is established.

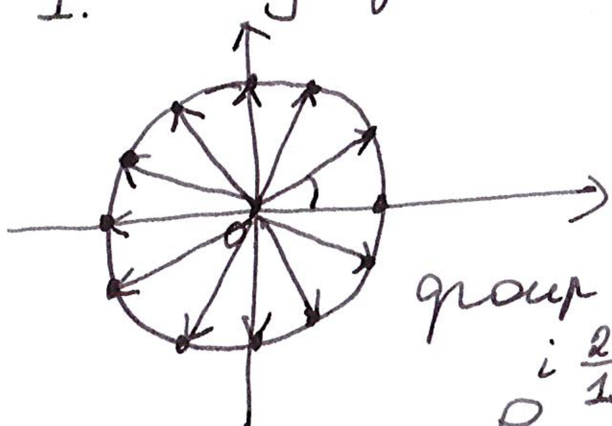
Now our aim is to prove uniqueness.

~~Theorem. Any two fields of order p^n are isomorphic.~~

But before that we will establish a very useful theorem (due to E. Galois).

<u>Theorem</u>. Let F be a field. Let G be a finite subgroup of the multiplicative group $F^* = (F \setminus \{0\}, \text{multiplication})$. Then the group G is cyclic.

<u>Example</u>. Let's consider the complex n-th roots of 1. They form a finite group



Here $n = 12$.

This is a cyclic group with generator $e^{i\frac{2\pi}{12}}$

Let's recall the theorem about finitely generated abelian groups.

Every finitely generated group is isomorphic to $C \times C \times \cdots \times C \times C_1 \times \cdots \times C_s$,

where $C \cong \mathbb{Z}$, infinite cyclic ~~gr~~ group, $C_i \cong \mathbb{Z}(n_i)$ cyclic group of order n_i, and $n_1 \mid n_2$, $n_2 \mid n_3, \ldots, n_{s-1} \mid n_s$.

The group G is finite, hence

$$G \cong C_1 \times \cdots \times C_s.$$

<u>Def</u>. The <u>exponent</u> of the group G is the smallest n such that $g^n = 1$ for an arbitrary element $g \in G$.

By Lagrange's Theorem $n \le |G|$.

<u>Question</u>: what is the exponent of

$C_1 \times \cdots \times C_s$?

<u>Answer</u>: n_s.

Indeed, consider an arbitrary element

$g = (g_1, \dots, g_s)$, $g_i \in C_i$. Then

$g^{n_s} = (g_1^{n_s}, g_2^{n_s}, \dots, g_s^{n_s})$. For every i, $1 \le i \le s$,

$g_i^{n_i} = e_i$, the identity of C_i.

But n_s is a multiple of n_i, hence

$g_i^{n_s} = e_i$ and $g^{n_s} = (e_1, e_2, \dots, e_s) = e$.

Is n_s the smallest? For any $1 \le k < n_s$

there exists an element $a \in C_s$ such

that $a^k \neq e_s$. Now

$(e_1, e_2, \dots, e_{s-1}, a)^k = (e_1, e_2, \dots, e_{s-1}, a^k) \neq e$.

We proved that $g^{n_s}=1$ for an arbitrary element $g\in G$. In other words all elements from G are roots of the equation $t^{n_s}-1=0$. The equation $t^{n_s}-1=0$ has $\leq n_s$ roots. Hence

$$|G|=n_1\cdots n_s\leq n_s.$$

It implies that $s=1$, i.e. the group G is cyclic, which completes the proof of the theorem.

Let F be a field of order p^n, $\operatorname{char} F=p>0$. The group $F^*=(F\setminus\{0\},\cdot)$ is cyclic. Let a be a generator of the group F^*.

Let $\mu_a(t)$ be the minimal polynomial over $\mathbb{Z}(p)$ of the element a. Recall that $\mu_a(a)=0$, the leading coefficient of $\mu_a(t)$ is $=1$ and $\mu_a(t)$ has the minimal degree among all polynomials over $\mathbb{Z}(p)$ with this property.

Recall also that if $f(t) \in \mathbb{Z}(p)[t]$ then $f(a) = 0$ if and only if $\mu_a(t) \mid f(t)$.

Indeed, if $f(t) = \mu_a(t)\, h(t)$ then $f(a) = \mu_a(a) \cdot h(a) = 0 \cdot h(a) = 0$.

Suppose that $f(a) = 0$. Divide $f(t)$ by $\mu_a(t)$ with a remainder:

$$f(t) = \mu_a(t)\, q(t) + r(t), \quad 0 \leq \deg r(t) < \deg \mu_a(t).$$

Then $0 = f(a) = \mu_a(a) \cdot q(a) + r(a)$, which implies $r(a) = 0$. This contradicts minimality of $\deg \mu_a(t)$.

<u>Lemma</u>. $\mathbb{Z}(p)[t] / (\mu_a(t)) \cong F$.

<u>Proof</u>. Consider the homomorphism

$$\mathbb{Z}(p)[t] \xrightarrow{\varphi} F, \quad f(t) \xrightarrow{\varphi} f(a).$$

this homomorphism is surjective since every nonzero element of F is a power of the element a.

What is $\ker\varphi$? A polynomial $f(t) \in \mathbb{Z}(p)[t]$ lies in $\ker\varphi$ if and only if $f(a) = 0$. We have seen above that $f(a)=0$ if and only if $\mu_a(t) \mid f(t)$. Hence,

$$\ker\varphi = (\mu_a(t))$$

By the Theorem about homomorphisms

$$\mathbb{Z}(p)[t] / (\mu_a(t)) \cong F. \quad \text{Ꚛ}$$

Let K be an algebraically closed field that contains the field $\mathbb{Z}(p)$ and such that the extension $K/\mathbb{Z}(p)$ is algebraic. We don't discuss uniqueness of K, we just choose one of such fields.

Since the field K is algebraically closed, the polynomial $\mu_a(t)$ has a root in K. Let $b \in K$, $\mu_a(b)=0$.

Consider the homomorphism

$$\mathbb{Z}(p)[t] \xrightarrow{\varphi} K, \quad f(t) \xrightarrow{\varphi} f(b).$$

Since $\mu_a(t) \xrightarrow{\varphi} \mu_a(b) = 0$ it follows that

$$(\mu_a(t)) \subseteq \ker\varphi.$$

Since $\mathbb{Z}(p)[t]/(\mu_a(t)) \cong F$ is a field, we conclude that $(\mu_a(t))$ is a maximal ideal of $\mathbb{Z}(p)[t]$. We have

$$(\mu_a(t)) \subseteq \ker\varphi \subseteq F[t].$$

The ideal $\ker\varphi$ can not be equal to $F[t]$ since $F[t]/\ker\varphi \neq (0)$. Hence,

$$\ker\varphi = (\mu_a(t)).$$

Let $Im(\Psi)$ be the image of the homomorphism Ψ. By the Theorem about homomorphisms

$$\mathbb{Z}(p)[t] / \ker \Psi \cong Im(\Psi)$$

On the other hand $\ker \Psi = (\mu_a(t))$ and $\mathbb{Z}(p)[t]/(\mu_a(t)) \cong F$. We proved that

$$F \cong Im(\Psi).$$

$Im(\Psi)$ is a subfield of K, $|Im(\Psi)| = p^n$. Every element from $Im(\Psi)$ is a root of the equation $t^{p^n} - t = 0$. Hence

$$Im(\Psi) = \{ k \in K \mid k^{p^n} - k = 0 \}.$$

We proved that an arbitrary field of order p^n is isomorphic to the subfield $\{k \in K \mid k^{p^n} - k = 0\}$ of the field K. This implies the following theorem.

<u>Theorem</u>. All fields of order p^n are isomorphic.

Public Cryptography.

Let p be a large prime number.

$\mathbb{Z}(p)^* = \{1, 2, \ldots, p-1\}$ is a cyclic group.

Let g be a generator of the group $\mathbb{Z}(p)^*$,

$\mathbb{Z}(p)^* = \{1, g, g^2, \ldots, g^{p-2}\}$

Alice $\longleftrightarrow$ Bob

Catherine (hacker)

<u>Diffie - Hellman scheme.</u>

Alice and Bob choose their secret numbers : m, n

$$g \to g^{m}, \quad (g^{m})^{n} = g^{mn}$$

$$g^{n} \leftarrow g$$

$$(g^{n})^{m} = g^{nm}$$

Both Alice and Bob share the secret:

$$g^{mn}$$

Catherine knows : g, g^{m}, g^{n}

The Problem of Discrete Algorithm.

AES (iPhones).

bit = 0, 1

bite = sequence of 8 bits

$\#(\text{bites}) = 2^{8} = 256$

There exists a finite field of order 256.

F^{*} = cyclic group of order 255.

4×4 matrix $(a_{ij})_{1 \le i,j \le 4}$, $a_{ij} \in F$

Elementary operations on rows and columns, + key, S-box

$$(a_{ij}) \to \left(\frac{1}{a_{ij}}\right).$$

What if $a_{ij} = 0$? $\frac{1}{0} = 0$.

why?

<u>Lagrange Theorem.</u> G finite group, $|G| = n$,

$a \in G$, $a^n = e$.

Then $a^{-1} = a^{n-1} = a^{254}$.

$254 = 2 \cdot 127$, $127 = 64 + 63$.

$$\underbrace{a \to a^2 \to a^4 \to a^8 \to a^{16} \to a^{32} \to a^{64}}_{\text{6 multiplications.}}$$

$63 = 7 \cdot 3 \cdot 3$

$$\underbrace{a \to a^7}_{6 \text{ mult.}} \longrightarrow (a^7)^3 \longrightarrow ((a^7)^3)^3$$

2 mult.

$$\underbrace{a^{64}}_{6 \text{ mult}} \cdot \underbrace{a^{63}}_{10 \text{ mult}}, \qquad \underbrace{a^{127} \cdot a^{127}}_{1 \text{ mult}}$$

Total: 17 multiplications.